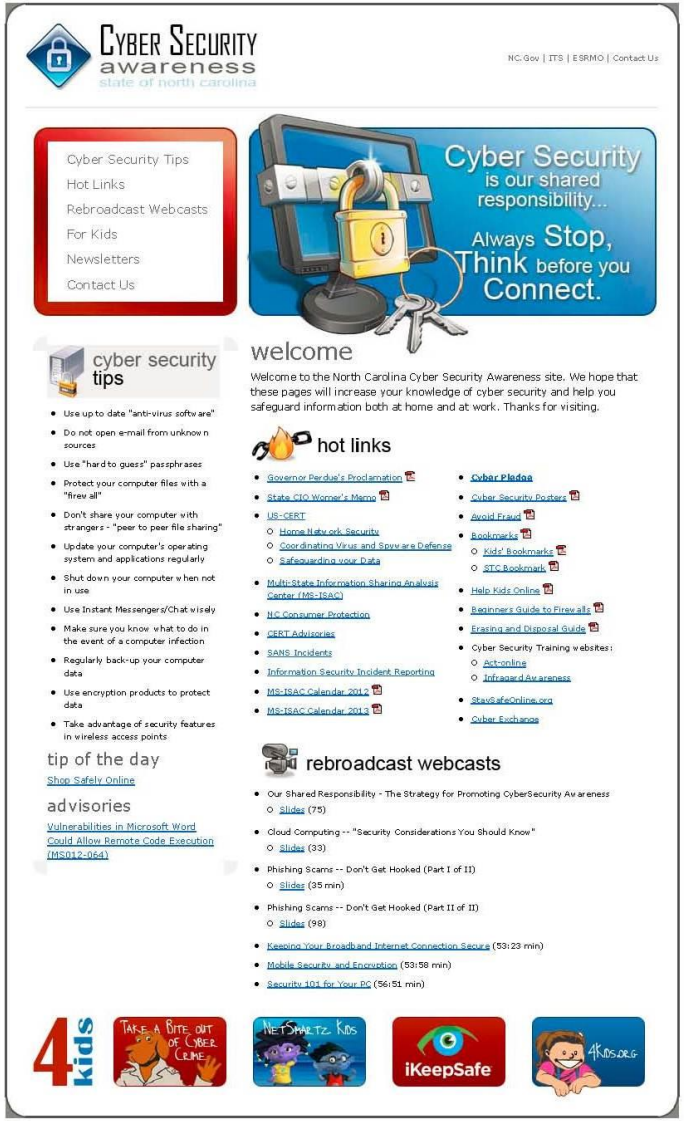
Statewide
Incident Response Review

"On the Internet, nobody knows you're a dog."

Cyber Security Awareness Website

- Contains useful information with helpful links
- The governor's proclamation is available to view
- Links for children and keeping them safer online
- Links to Free Security Training (*i.e. no cost)*
- Website address is:

http://www.esrmo.scio.nc.gov/CyberSecurity/default.aspx



Cyber Security Pledge

- Stop, and Think (consider appropriateness and risk) before I Connect to the Internet.
- Take personal responsibility for security, follow my agency's security policies.
- Work to the best of my ability to keep my agency's staff, property and information safe and secure.
- Promptly report all security incidents or concerns to my organization's security office or other appropriate contact.
- Spread the message to my friends, co-workers and community about staying safe online.
- Website address is: http://www.esrmo.scio.nc.gov/CyberSecurity/default.aspx

Cyber Security: What is it?

- **<u>Cyber Security (computer security)</u>** is a branch of information security that applies to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, unauthorized access, or natural disaster, while allowing the information and property to remain accessible and productive to the intended users.

Security Incident

An information security incident is an **adverse** event or a threat of an adverse event where an information technology resource is:

- Accessed or used without authorization
- Attacked or threatened with attack
- Used in a manner inconsistent with established laws or policy with the potential to cause the real or possible loss of *confidentiality, integrity, or availability* of the resource or its information
- Breached or threatens to breach the accountability, or auditability of the resource or its information.

Reportable Incidents

E-Mail

- SPAM
- Open Relay Complaints
- DOS against Mail servers
- E-mail Harassment
- Spam BOT
- Phishing (Social Engineering)

Reportable Incidents

Hacking

- Port scanning
- Unauthorized access
- SQL Injection
- Warez Servers
- Anonymous Proxies
- Web Defacements
- Denial of Service (DOS)
- Brute Force Attacks
- System Compromise

Reportable Incidents

Malicious Software (aka. Malware)

- Malware Outbreaks
  - Multiple systems/users reporting infection
- AV Failures (Large Scale)
  - Fail to detect
  - Fail to clean
- Vectors of Infection
  - Hostile websites
  - Malicious email/text/social networking links

Reportable Incidents

Inappropriate Use

- Copyright violations (Peer-to-Peer Networks – Kaaza, Gnutella, Torrents)
- Downloading and/or distribution of pornography
- Unauthorized access to remote system/account by state employee
- Use of state resources for personal gain or harassment

Reportable Incidents

Other

- Law Enforcement Issues
  - Intelligence
  - Theft and Fraud
  - Stalking
  - Harassing Telephone Calls
- Data loss (Desktops, laptops, portable media, etc.)
  - *When reporting these incidents, you must note if the device and/or media contained PII and if the device/data was protected with encryption.*
- Miscellaneous incidents not covered above!

Agency Responsibilities

G.S.§ 147-33.113(a) requires agency heads to:

- Provide details of information technology security employed at the agencies
- Report computer related security incidents to the State CIO within 24 hours
- Designate an agency security liaison to coordinate with the State CIO

The General Assembly, Judicial Department, and the University of North Carolina system are exempt, but may choose to comply.

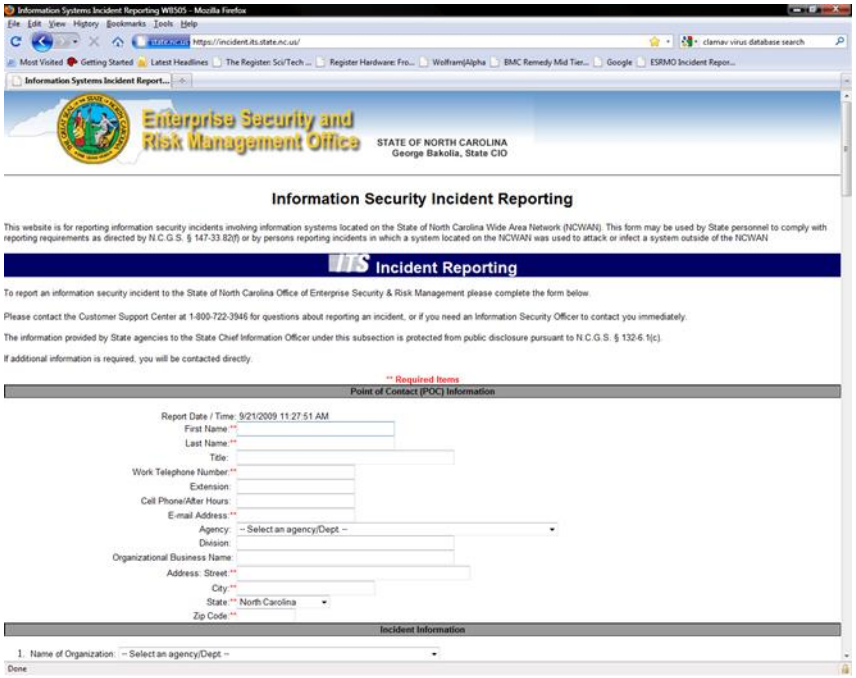
How do I report an incident?

- Three Methods for reporting cyber incidents:
  - Report the incident using the online incident reporting form at https://incident.its.state.nc.us *
  - Open a ticket with the ITS Service Desk *
    - Ask for it to be routed to ESRMO/Threat Management
  - Contact a member of the ESRMO Threat Management Team directly

**If you need immediate assistance, please contact a member of the Threat Management team directly.*

How do I report an incident?

- Report cyber incidents at https://incident.its.state.nc.us
- What ESRMO submits on the agency's behalf:
  - Malware notifications ESRMO sends to the agency
  - Spam notifications ESRMO sends to the agency
  - Copyright Infringement notifications ESRMO sends to the agency



- All other cyber incidents should be submitted by the agency.

Questions?